AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for providing secure transmissions across a network comprising a ~~transmitting device~~ client device and a ~~receiving device~~ server, the method comprising:

at the ~~transmitting device~~ client device, generating a stream of watermark bits;

generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;

inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets;

receiving, at the ~~receiving device~~ server, the plurality of outgoing packets; and

determining if a received packet is valid based on the watermark in the header of the received packet.

2. (Currently Amended) The method of claim 1, wherein generating the stream of watermark bits includes generating a stream of watermark bits from an authorization and ~~sychronization~~ synchronization packet previously exchanged between the ~~transmitting device~~ client device and the ~~receiving device~~ server.

3. (Currently Amended) The method of claim 1, further comprising activating a session by exchanging an authorization and synchronization packet between the ~~transmitting device~~ client device and the ~~receiving device~~ server.

4. (Original) The method of claim 1, further comprising:

discarding the packet, if the watermark is not valid.

5. (Original) The method of claim 1, wherein determining if a received packet is valid comprises:

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and

accepting the watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

6. (Currently Amended) The method of claim 5, wherein the set of expected watermarks are generated from an authorization and ~~sychronization~~ synchronization packet previously exchanged between the ~~transmitting device~~ client device and the ~~receiving device~~ server.

7. (Original) The method of claim 5, comprising:

discarding the packet, if the watermark does not match one in the first or second windows.

8. (Currently Amended) The method of claim 5, wherein comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-numbered valid watermark received from the ~~transmitting device~~ client device;

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks and wherein the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately ~~supercede~~ supersede the pivotal index number.

9. (Original) The method of claim 8, comprising:

increasing the pivotal index number if a match is found in the second window and deleting the matching expected watermark from the second window.

10. (Original) The method of claim 1, wherein the stream of watermark bits is generated by a stream cipher.

11. (Original) The method of claim 1, wherein inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

12. (Currently Amended) A system for providing secure transmissions across a network, the comprising:

a ~~transmitting device~~ client device for

generating a stream of watermark bits;

generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;

inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets; and transmitting the outgoing packets to a ~~receiving device~~ server; and

a ~~receiving device~~ server for

receiving the plurality of outgoing packets; and

determining if a received packet is valid based on the watermark in the header of the received packet.

13. (Currently Amended) The system of claim 12, wherein the stream of watermark bits are generated from an authorization and synchronization packet previously exchanged between the ~~transmitting device~~ client device and the ~~receiving device~~ server.

14. (Original) The system of claim 12, wherein inserting at least one of the plurality of watermarks includes determining whether a valid session exists and inserting the at least one of the plurality of watermarks only if the valid session exists.

15. (Currently Amended) The system of claim 12, wherein the ~~receiving device~~ server further discards the packet, if the watermark is not valid.

16. (Currently Amended) The system of claim 12, wherein the ~~receiving device~~ server further determines if a received packet is valid by the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks; and

accepting the received watermark as valid if the received watermark matches one of the expected watermarks in the first or second windows.

17. (Currently Amended) The system of claim 16, wherein the ~~receiving device~~ server further discards the packet, if the received watermark does not match any expected watermarks in the first or second windows.

18. (Currently Amended) The system of claim 16, wherein comparing the watermark further comprises:

maintaining at the server a record of a pivotal index number representing the index number of the highest-numbered valid watermark received from the ~~transmitting device~~ client device;

comparing the watermark of the received packet to a first and a second window, each of the windows comprising a set of expected watermarks and wherein the first window represents expected watermarks whose index numbers precede the pivotal index number and the second window represents expected watermarks whose index numbers immediately ~~supercede~~ supersede the pivotal index number.

19. (Currently Amended) The system of claim ~~17~~ 18, wherein the ~~receiving device~~ server increases the pivotal index number if a match is found in the second window and deletes the matching expected watermark from the second window.

20. (Original) The method of claim 12, wherein the stream of watermark bits is generated by a stream cipher.

21. (Currently Amended) A system for providing secure transmissions across a network from a client device to a server, the system comprising:

means for generating a stream of watermark bits;

means for generating a plurality of watermarks, each of the plurality of watermarks comprising an index number and a portion of the stream of watermark bits;

means for inserting at least one of the plurality of watermarks into each header of a plurality of outgoing packets; and

means for transmitting the outgoing packets to a ~~receiving device~~ server capable of determining if a received packet is valid based on the watermark in the header of the received packet.